



iPECS-CM

Security Configuration Manual

Please read this manual carefully before operating System.
Retain it for future reference.

iPECS is an Ericsson-LG Brand



Revision History

ISSUE	DATE	DESCRIPTION OF CHANGES
1.0	15-Apr-14	Initial Release

Copyright© 2014 Ericsson-LG Enterprise Co., Ltd. All Rights Reserved

This material is copyrighted by Ericsson-LG Enterprise Co., Ltd. (Ericsson-LG Enterprise). Any unauthorized reproductions, use or disclosure of this material, or any part thereof, is strictly prohibited and is a violation of Copyright Laws. Ericsson-LG Enterprise reserves the right to make changes in specifications at any time without notice. The information furnished by Ericsson-LG Enterprise in this material is believed to be accurate and reliable, but is not warranted to be true in all cases. If you are not the intended recipient, you should destroy or retrieve this material to Ericsson-LG Enterprise.

iPECS is trademark of Ericsson-LG Enterprise Co., Ltd.

All other brand and product names are trademarks or registered trademarks of their respective companies.

Table of Contents

1	WHY SECURITY CONFIGURATION IS REQUIRED!	1
2	SECURITY CONFIGURATION IN CENTOS	2
2.1	CHANGE ROOT AND USER PASSWORD	2
2.2	CONFIGURING ACL OF SSH	2
2.3	CHANGE SAMBA PASSWORD	3
2.4	CONFIGURING ACL OF SAMBA	4
3	CHANGE WMS PASSWORD	5
4	ACL SETTINGS ON WMS	6
4.1	SETTING ACL LISTS	6
4.2	APPLYING ACL RULES	7
4.3	APPLICATION OF WAN/LAN NETWORK	8
5	RESTRICTION OF SIP REGISTRATION	9
5.1	SIP RESTRICTION MANAGEMENT	9
5.2	SIP RESTRICTION INFORMATION	10
5.3	AUTHENTICATION PASSWORD SETTING OF SIP PHONE	11
5.4	407 AUTHENTICATION SETTING OF SIP PHONE	12
5.5	ACCESS RESTRICTION FOR INDIVIDUAL USER	13
5.6	DELETION UNUSED SIP ACCOUNT	13
6	HTTPS SETTING	14
7	DISA SETTINGS	15

1 Why security configuration is required!

When the system is connected to the public network, it's vulnerable to the hacking for the malicious purpose. If the root password is cracked or leaked, the system can be infected by any computer virus or backdoor program . In this case the system can be reset during operation or voice quality may be affected by high traffic of the hidden program.

To protect this malicious access to the system, it's required to change default password and restrict access from unauthorized IP address.

This document explain how to change settings regarding security options such as:

- Security options in CentOS
- Security options in WMS
- Security options for SIP Signaling

It's strongly recommended to change the following passwords and IP filtering rule in the installation stage.

- Root password of shell login
- Samba password
- WMS password
- IP Filtering for ssh, samba service

Even after configuring ACL(Access Control List) in CM system by WMS & Linux OS Command and changing above Default password with Strong password, CM system can't protect Flooding & DDoS Attack and CM System may can't operate properly. So, the installation of Firewall and SBC device is also strongly recommended.

2 Security configuration in CentOS

2.1 Change root and user password

This chapter explains how to change system password for the protection from illegal access. It's very strongly recommended that the new password is set on the condition of the followings.

Recommendations for strong password :

- 1) It should be at least 9 characters.
- 2) It should include 3 or more types of the following categories.
: uppercase letters, lowercase letters, number, and special character
- 3) It should not contain user name and real name and company name.
- 4) It should not contain a complete word.
- 5) It should not include same or sequential numbers (ex, 123..., 111..., abc....)

[Notice] Please be careful not to forget new password.

To change password

- 1) Connect to the server through SSH as a root
- 2) Change "root" password

root@CentOS58 /root \$ passwd	→ Type This command
<i>Changing password for user root.</i>	
<i>New UNIX password:</i>	→ <i>Type "strong password"</i>
<i>Retype new UNIX password:</i>	→ <i>Confirm the password</i>
<i>passwd: all authentication tokens updated successfully.</i>	

- 3) change "ipeccsm" user password

root@CentOS58 /root \$ passwd ipecscm	→ Type This command
<i>Changing password for user ipecscm.</i>	
<i>New UNIX password:</i>	→ <i>Type "strong password"</i>
<i>Retype new UNIX password:</i>	→ <i>Confirm the password</i>
<i>passwd: all authentication tokens updated successfully.</i>	

2.2 Configuring ACL of SSH

Networking **access control list**(ACL) is a list of permission to access to the system. It allows only listed IP address to connect to the system and it can prevent illegal access to the system from any unauthorized IP address.

The **TCP wrapper** is running on the system and it works as a firewall to prevent the malicious access.

SSH IP Filtering

- 1) Connect to the server through SSH as a root
- 2) Edit deny rules

- A. Open deny configuration file (/etc/hosts.deny)
: If it finds a matching rule, it denies the connection
- B. Add this line, "sshd:ALL"
: All packet for SSH connection will be dropped.

```
root@CentOS58 ~ $ vim /etc/hosts.deny
sshd:ALL
```

Notice) Please keep in mind to assign the IP address of management PC to allow list. If any IP is not defined in allow list, all the connection will be rejected. The ACL rule would be applied from new session.

- 3) Edit allow rules
 - A. Open allow configuration file (/etc/hosts.allow)
: If it finds a matching rule, it accept the connection
 - B. Add this line, "sshd:<authorized IP>"
: SSH connection will be accepted only from the authorized IP address.

ex1) only 1 IP allow: 192.168.122.190

```
root@CentOS58 ~ $ vim /etc/hosts.allow
sshd:192.168.122.190
```

ex2) Two IP allow: 192.168.122.190, 192.168.122.191

```
root@CentOS58 ~ $ vim /etc/hosts.allow
sshd:192.168.122.190, 192.168.122.191
```

ex3) Local Subnet allow: 192.168.122.0/24

```
root@CentOS58 ~ $ vim /etc/hosts.allow
sshd:192.168.122. ← it contains period at the end position.
```

2.3 Change SAMBA password

This chapter explains how to change password of SAMBA for accessing from Windows PC.

Refer to Chapter 2.1 for the strong password.

To change password

- 1) Connect to the server through SSH as a root
- 2) Change password

```
root@CentOS58 ~ $ smbpasswd -a ipecscm → Type this command
New SMB password: → Type "strong password"
Retype new SMB password: → confirm the password
```

2.4 Configuring ACL of SAMBA

This chapter explains how to configure authorized IP address of SAMBA for accessing to the system directory from Windows PC.

SAMBA IP Filtering

- 1) Edit allow rules
 - A. Open allow configuration file (/etc/samba/smb.conf)
 - B. Find the line "# hosts allow =" in the "[global]" section, and edit this line
 - C. Remove #, # means omitting this line when the samba service is initialized.
: The packet for Samba connection from authorized IP will be accepted.

ex1) only 1 IP allow: 192.168.122.190

```
root@CentOS58 ~ $ vim /etc/samba/smb.conf
hosts allow = 192.168.122.190
```

ex2) Two IP allow: 192.168.122.190, 192.168.122.191

```
root@CentOS58 ~ $ vim /etc/samba/smb.conf
hosts allow = 192.168.122.190 192.168.122.191
```

ex3) Local Subnet allow: 192.168.122.0/24

```
root@CentOS58 ~ $ vim /etc/samba/smb.conf
hosts allow = 192.168.122.    ← it contains period at the end position.
```

SAMBA Service Restart

For applying these configuration, the samba service should be restarted.

- 1) Connect to the server through SSH as a root
- 2) Type the following command to restart SAMBA service

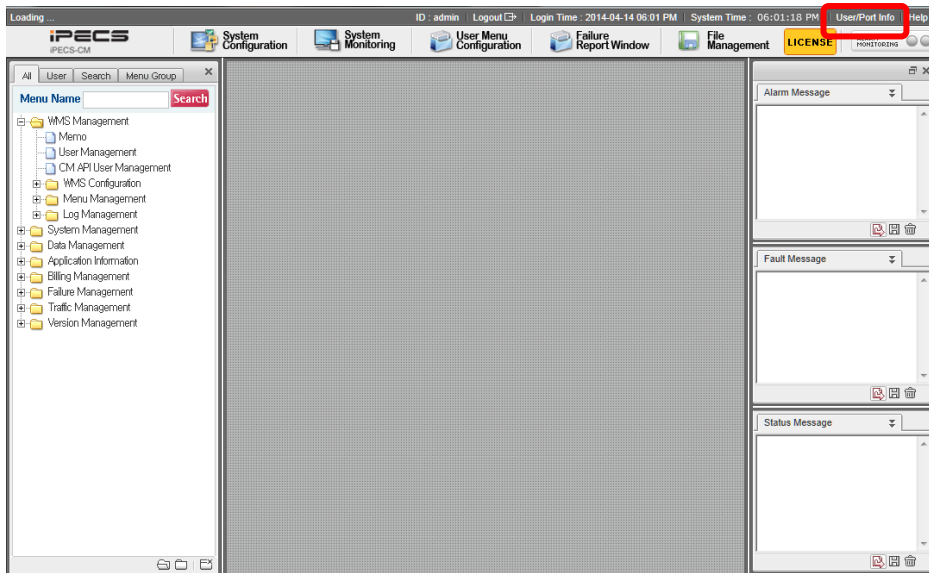
```
root@CentOS58 ~ $ service smb restart
```

3 Change WMS Password

It's strongly recommended to change default password of WMS to protect the system and user data.

To change password

- 1) After login Admin & Maintenance account, you can change the password in User/Port Info menu of the upper right.
- 2) When you change the password, it requires strong password as follows from version 5.5.
When you login at the first time to the WMS, it requires to change password.
 - A. The length should be at least 9 characters.
 - B. It should contains 3 or more types of the categories.
: uppercase letters, lowercase letters, number, and special character
 - C. It should not include 3 serial number of serial same number (ex, 123..., 111..., abc....).



User/Port Info

Load Modify Close

Division	ID	Password	HTTP Port	HTTPS Port
Current Value	admin	*****	80	443
Change Value				

Email:

Phone No.:

Mobile No.:

※ Reference

1. If you change ID / Password / WebPort, it is to logout automatically.
2. After change ID / Password, Try to login new ID / Password.
3. If you change WebPort, server is restarted automatically.

- After one more minutes, you can access to WMS include new WebPort.
- Example: http://xxx.xxx.xxx.xxx:xxxx

HTTP Service		
Usage	Type	Port
Use	HTTPS	7878

Process Success!

4 ACL Settings on WMS

4.1 Setting ACL lists

It's explained how to configure access restriction of SSH and SAMBA in Chapter 2. This chapter explains how to reject the other protocols in addition.

ACL in WMS works based on white list and all the services are restricted except one defined to use on the menu below.

To Set ACL in WMS

- 1) Login with admin account to WMS to set ACL list, user account can't access to the menu.
: System Management → ACL Information
- 2) Press "Add" button to add new rule.
- 3) Input the following data.
 - A. Enter individual IP address or IP range.
 - B. Select coverage. LAN or WAN
 - C. Select the "Service All" option.

If you want to use specific protocol, set "Service All" to "Use Part" and select protocol.

 ACL Information > Add

IP Address	192.168.122.0/24	LAN / WAN	LAN
Service All	Use All	Description	

Service Name	Protocol	Port	Usage
ICMP	ICMP	0	Not Use
TELNET	TCP	23	Not Use
SSH	TCP	22	Not Use
FTP	TCP	1022	Not Use
HTTP	TCP	80	Not Use
SNMP	UDP	161	Not Use
	TCP		Not Use
	TCP		Not Use
	TCP		Not Use
	TCP		Not Use

To check ACL with CLI

- 1) Connect to the server through SSH as a root
- 2) Type command "iptables -L"
- 3) The following line will be added in the location "Chain INPUT"
ACCEPT all -- 192.168.122.0/24 anywhere

```
root@CentOS58 ~ $ iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT    all  --  192.168.122.0/24      anywhere
```

Cautions

- If you use ACL settings without any allowed IP address, all the access from any G/W, IP phone, PC is denied.
- When access from OAM PC is restricted, you have to delete ACL list with CLI (console command)

```
root@CentOS58 ~ $ iptables -F INPUT ACCEPT
```

4.2 Applying ACL rules

This chapter explains how to apply ACL rules defined in WMS. If ACL option is set to "Use", all the services will be rejected except that defined to use in Chapter 4.1.

To Apply ACL in WMS

- 1) When you complete to set the ACL list, select ACL option "Use" to apply the ACL rules.
: System Management → System Environment -> ACL(Access Control List)

The screenshot shows a window titled "System Environment" with a table of configuration options. The "ACL(Access Control List)" option is highlighted with a red box and is set to "Use".

Country code	Korea
System Name	
Number of Tenant in System	1
System Numbering Plan	System Base
Extension default password(0000) Use	Not Use
Free Zone Digit Info Use	Not Use
Dual CM IP Profile Use	Use
ACL(Access Control List)	Use
Min. Communication Level	Not Use
Geographical Dual Use	Not Use
Terminal CID Password	****
Area Number	
Input Digits of Command Call Group No.	2 Digits
Hosted Service Use	Not Use
GW FW Upgrade Use	Use

Process Success!

To check ACL option with CLI

- 1) Connect to the server through SSH as a root
- 2) Type command "iptables -L"

```
root@CentOS58 ~ $ iptables -L
Chain INPUT (policy DROP) → If it's "DROP", it means "Not Use".
```

```
root@CentOS58 ~ $ iptables -L
Chain INPUT (policy ACCEPT)  → If it's "ACCEPT", it means "Use".
```

4.3 Application of WAN/LAN Network

You can set to not apply the ACL for the device which is connected to LAN port
Access from WAN is restricted but only access from LAN is allowed

ACL Information									
Load Modify Add Del Close									
									Total Count 2
☒	Move	Index	IP Address	LAN/ WAN	Service All	Description	Service (Service Name/Protocol/Port/Usage)		
☐		1	192.168.0.0/16	LAN	Use All		ICMP	0	Not Use
							TELNET	23	Not Use
							SSH	22	Not Use
							FTP	1022	Not Use
							HTTP	80	Not Use
							SNMP	161	Not Use
							ICMP		Not Use
							ICMP		Not Use

5 Restriction of SIP Registration

5.1 SIP Restriction Management

iPECS-CM supports to restrict any illegal access or flooding attack of SIP message.

Blocking based on ACL

SIP signaling is allowed based on ACL configuration, so it require to set ACL options. All the terminal IP address should be contained in ACL allow list. ACL setting is referred in chapter 4.1 and chapter 4.2.

Blocking based on IP address

1) SIP Message Block Mode

- All SIP Message Blocked : If IP address of current message is different with the IP address previously received, the REGISTER message is dropped and any message is not responded.
- All SIP Message Blocked Except REGISTER : If IP address of current message is different with the IP address previously received, only REGISTER message is allowed and other messages are dropped.
- All SIP Message Allowed
Allow all messages to receive.

2) Register Message Author Retry Count : 10~100, default value is 30

When Registration Request fail count is over this value with the reason of password mismatch or undefined number, the IP address is restricted. You can check the restricted IP address on the menu "SIP Restriction Information".

3) SIP Restriction Count for Registration(sec) : 1~200, default is 10.

This option is for checking REGISTER flooding. If REGISTER message is flooded more than this count in a second, the IP address is added to restriction list. You can check the restricted IP address on the menu "SIP Restriction Information".



5.2 SIP Restriction Information

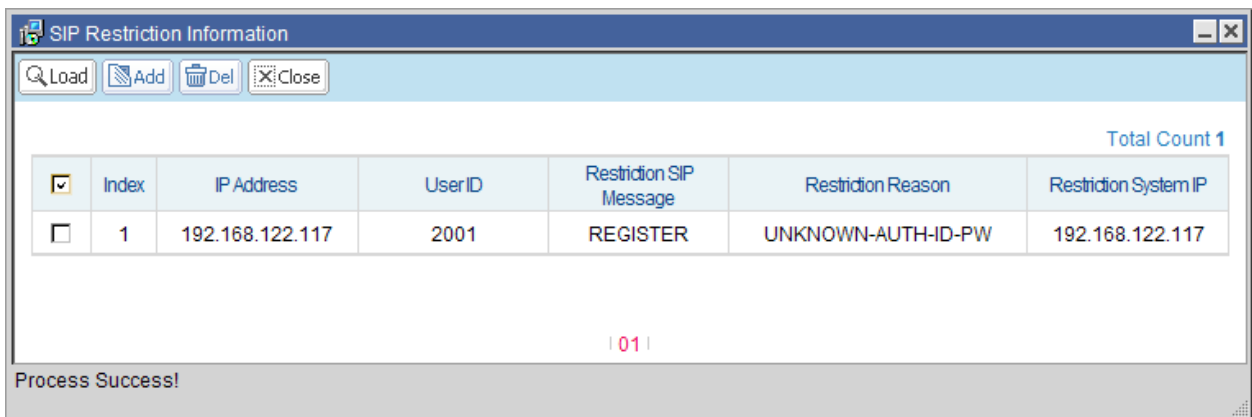
This menu shows the restricted IP addresses with the reason. The administration can release the restricted IP address with deleting from the list.

Restriction Reason

- Unknown IP : The IP of the terminal is different with first registered.
- Unknown user ID : User ID is not defined.
- Unknown auth ID/PW : Password mismatch
- Terminal type mismatch : The User-Agent and terminal type is not matched.
- Heavy Traffic : It's restricted by SIP flooding

Caution

- 1) If specific SIP phone fails to register to the system, please check the IP is restricted.
- 2) If the terminal is behind NAT or LCM, please use “All SIP Message Blocked Except REGISTER” instead of “All SIP Message Blocked”



The screenshot shows a web application window titled "SIP Restriction Information". It contains a toolbar with "Load", "Add", "Del", and "Close" buttons. Below the toolbar is a table with the following columns: Index, IP Address, UserID, Restriction SIP Message, Restriction Reason, and Restriction System IP. The table has one data row with the following values: Index 1, IP Address 192.168.122.117, UserID 2001, Restriction SIP Message REGISTER, Restriction Reason UNKNOWN-AUTH-ID-PW, and Restriction System IP 192.168.122.117. The table is also labeled with "Total Count 1". Below the table, there is a status bar that says "Process Success!".

☒	Index	IP Address	UserID	Restriction SIP Message	Restriction Reason	Restriction System IP
☐	1	192.168.122.117	2001	REGISTER	UNKNOWN-AUTH-ID-PW	192.168.122.117

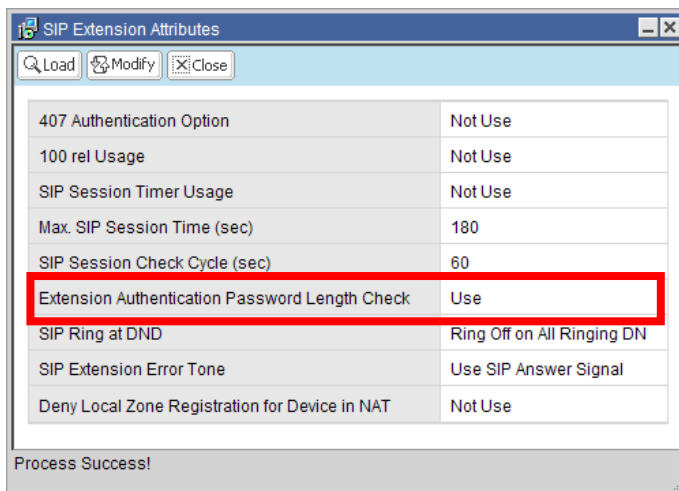
| 01 |

Process Success!

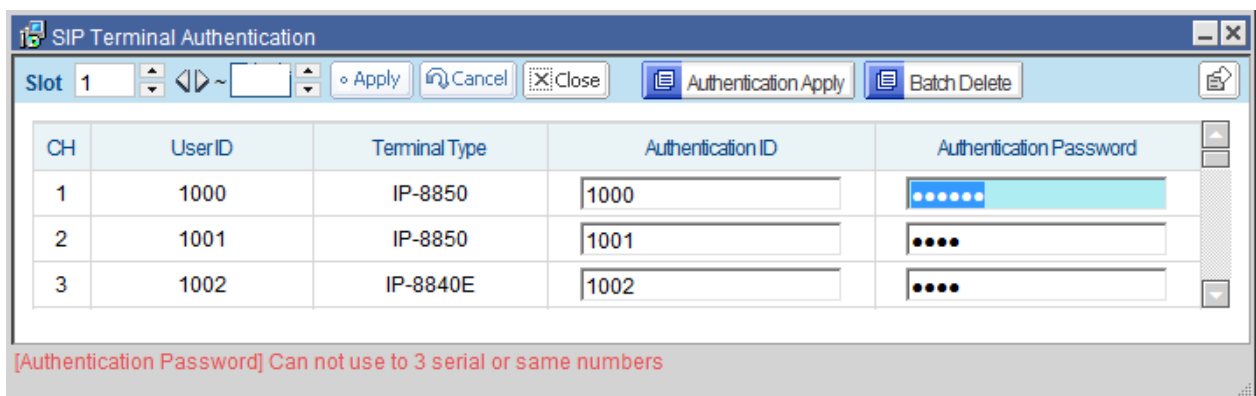
5.3 Authentication password setting of SIP phone

It's recommended to use strong password for SIP authentication password. When the following option is enabled, the system will check if password is valid or not depending on the following conditions.

- The length should be at least 6 characters.
- It should contains 3 or more types of the categories.
: uppercase letters, lowercase letters, number, and special character
- It should not include 3 serial number of serial same number (ex, 123..., 111..., abc....).
- Never use a password same as station number or user id.

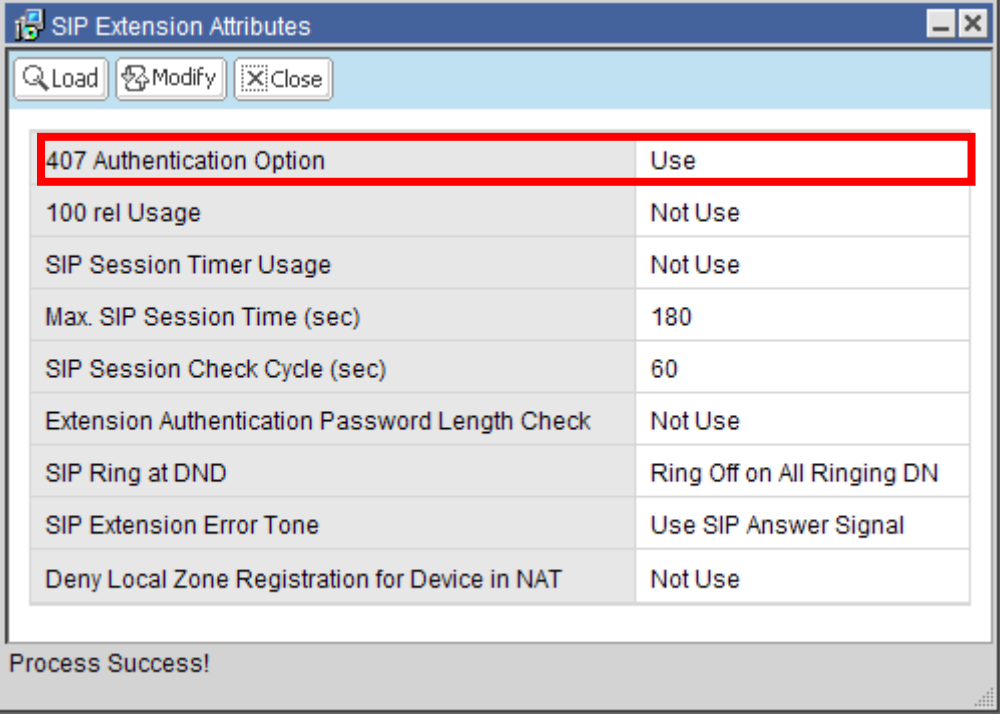


Ex) Sequential number is denied.



5.4 407 Authentication setting of SIP phone

It's recommended to set "407 Authentication Option" to "Use" for checking authentication for all the outgoing calls. If it's set to "Use", iPECS-CM will send 407 for Invite request.



The screenshot shows a window titled "SIP Extension Attributes" with a toolbar containing "Load", "Modify", and "Close" buttons. Below the toolbar is a table with the following settings:

407 Authentication Option	Use
100 rel Usage	Not Use
SIP Session Timer Usage	Not Use
Max. SIP Session Time (sec)	180
SIP Session Check Cycle (sec)	60
Extension Authentication Password Length Check	Not Use
SIP Ring at DND	Ring Off on All Ringing DN
SIP Extension Error Tone	Use SIP Answer Signal
Deny Local Zone Registration for Device in NAT	Not Use

At the bottom of the window, a status bar displays the message "Process Success!".

5.5 Access restriction for individual user

iPECS-CM supports that users change their own data of call features from Web admin. But if it's not necessary, change any individual users not to allow to the Web admin. Or change not to use default password for Web admin.

- Restrict individual user web access
Set "Max Login User of Extension User Web" of "WMS Basic Configuration" to "0."
- Don't use default password
Set "Extension default password(0000) Use" of "System Environment" to "Not Use"

WMS Basic Configuration

Basic Set Functional Set

Setting Item	Setting Value
Language Setting(Basic)	Korean
Security Setting(IP Filtering)	Not Use
Max Count of Data Modification History	1000
Removal Count of Data Modification History	100
Max Count of Login History	1000
Removal Count of Login History	100
Max Login User of Extension User Web	0
Max Login User of Administrator Web	5
Followings are applied for Administrator Web.	
Auto Logout by Idle Time	Not Use
Auto Logout Time(Minute)	
Max Length for Password	6
Password Mix (Number, English, Special Letter)	Mix over 2 Kinds
Check Term for Change Password	Not Use 3 Month(s)
Login Retry Check	Not Use
Login Retry Count	
Login Retry Time	10 Minutes
Authority Function on Menu	Not Use

Process Success!

System Environment

Apply Cancel Close

Country code	Korea
System Name	
Number of Tenant in System	10
System Numbering Plan	System Base
Extension default password(0000) Use	Use
Free Zone Digit Info Use	Not Use
Dual CM IP Profile Use	Use
ACL(Access Control List)	Not Use
Min. Communication Level	Not Use
Geographical Dual Use	Not Use
Terminal CID Password	
Area Number	
Input Digits of Command Call Group No.	2 Digits
Hosted Service Use	Not Use
GW FW Upgrade Use	Use

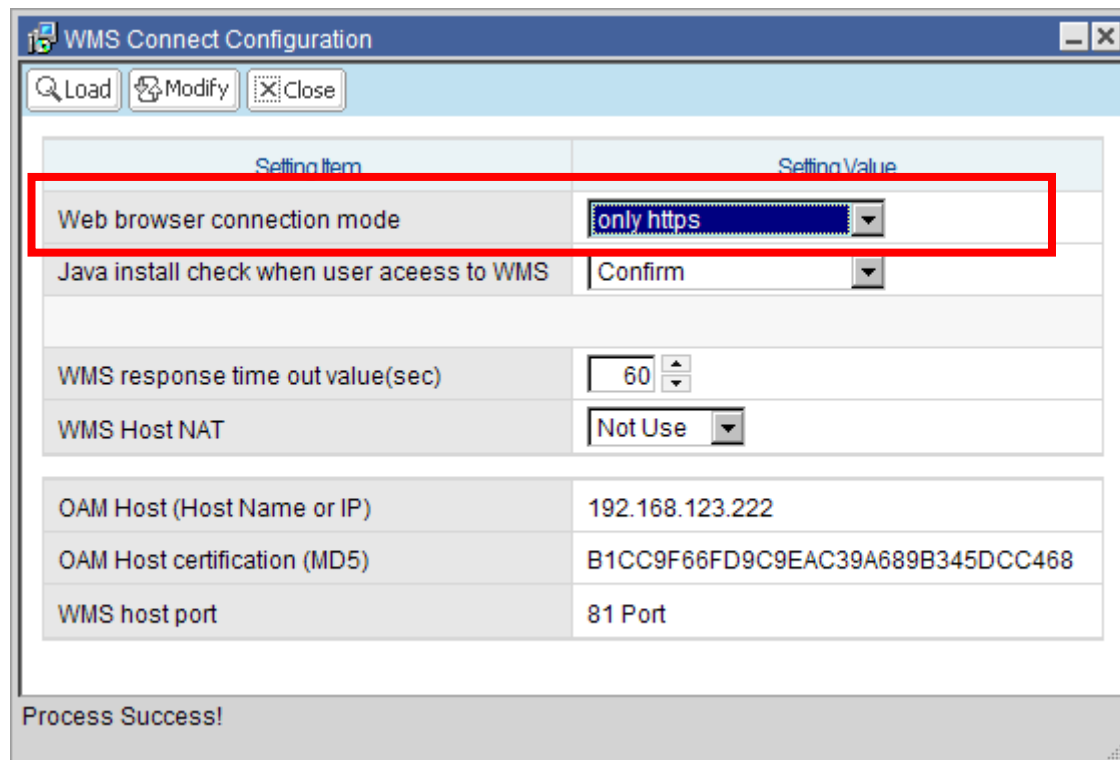
Process Success!

5.6 Deletion unused SIP account

It's recommended not to create unused SIP account for prevent hacking. If the user id and password is leaked, it can be used maliciously.

6 HTTPS Setting

When system use https, connect to "https://xxx.xxx.xxx.xxx/" to access WMS.



The image shows a 'WMS Connect Configuration' window with a toolbar containing 'Load', 'Modify', and 'Close' buttons. Below the toolbar is a table with two columns: 'Setting Item' and 'Setting Value'. The first row, 'Web browser connection mode', is highlighted with a red box and has a value of 'only https'. The second row, 'Java install check when user access to WMS', has a value of 'Confirm'. The third row, 'WMS response time out value(sec)', has a value of '60'. The fourth row, 'WMS Host NAT', has a value of 'Not Use'. The fifth row, 'OAM Host (Host Name or IP)', has a value of '192.168.123.222'. The sixth row, 'OAM Host certification (MD5)', has a value of 'B1CC9F66FD9C9EAC39A689B345DCC468'. The seventh row, 'WMS host port', has a value of '81 Port'. At the bottom of the window, a status bar displays 'Process Success!'.

Setting Item	Setting Value
Web browser connection mode	only https
Java install check when user access to WMS	Confirm
WMS response time out value(sec)	60
WMS Host NAT	Not Use
OAM Host (Host Name or IP)	192.168.123.222
OAM Host certification (MD5)	B1CC9F66FD9C9EAC39A689B345DCC468
WMS host port	81 Port

Process Success!

7 DISA settings

DISA(Direct Inward System Access) is used for external subscriber to use DDD/ISD call through system access, but if not use DISA feature set "DISA Transit" to "Deny" or "Authorization for DISA Transit" to "Use"

Route Number	1	Type	Day	Load	Modify	Close
Trunk Call Routing Table	2					
DISA Transit	Deny					
Authorization for DISA Transit	Use					
DISA Retry Count	3					
Multi Ring No Answer Time (sec)	0					
Trunk Call Routing Table for Multi Ring No Answer						

Process Success!